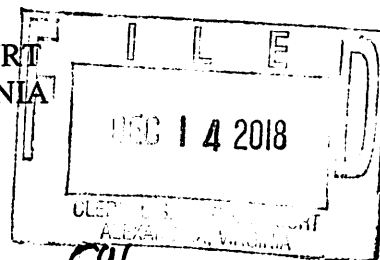


IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



UNITED STATES OF AMERICA)

v.)

PAUL J. WILSON,)

Defendant.)

CASE NO. 1:18-MJ-

UNDER SEAL

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, Ted P. Delacourt, a Special Agent with the Federal Bureau of Investigation (FBI),
Washington Field Division, Washington, D.C., being duly sworn, depose and state as follows:

INTRODUCTION

1. Your Affiant has been employed by the FBI since September of 2004, and as a Special Agent since September 2005. Since 2005, I have received training and experience in interviewing and interrogation techniques, and arrest and search procedures. I was assigned as a Special Agent in the Jacksonville Division in January 2006, where I worked counterterrorism and intelligence-gathering operations for approximately three years. I was assigned to the Washington Field Office in May 2009 and charged with investigating international corruption, specifically violations of the Foreign Corrupt Practices Act (FCPA), as well as antitrust violations. In January 2009, I was promoted to Supervisory Special Agent and assigned to the Counterterrorism Division of FBI Headquarters, specifically to the National Joint Terrorism Task Force. In August 2012, I transferred within the Counterterrorism Division to the International Operations Section I, Continental US Unit V, where I program managed International Terrorism investigations in the Phoenix Division. I am currently assigned to the Washington Field Office, Northern Virginia Resident Agency, Child Exploitation Task Force. Since joining the FBI, I

have investigated violations of federal law. As a federal agent, I am authorized to investigate violation of laws of the United States and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States. Since September 2014, I have been assigned to investigate violations of law concerning the sexual exploitation of children, including child pornography and child sex trafficking. I have gained experience through both formal and on-the-job training in conducting these types of investigations.

2. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, which includes conversations with law enforcement officers and others, and review of reports and database records. For the purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that between on or about April 21, 2013 and on or about July 15, 2015, within the Eastern District of Virginia and elsewhere, PAUL J. WILSON violated Title 18, United States Code, Sections 2252(a)(1) and (b)(1) and 2, by transporting child pornography or causing it to be transported from Washington, D.C. to Annandale, Virginia.

4. Because this affidavit is being submitted for the limited purpose of securing an arrest warrant, I have not included each and every fact known to me concerning this investigation. I have included only those deemed necessary to demonstrate probable cause that Wilson committed the offense alleged in this complaint.

STATUTORY AUTHORITY AND DEFINITIONS

5. Title 18, United States Code, Section 2252(a)(1) and (b)(1) prohibits the knowing transportation or shipment of any visual depiction of minors engaging in sexually explicit

conduct using any means or facility of interstate or foreign commerce or in or affecting interstate commerce by any means, including by computer.

6. Title 18, United States Code, Section 2 provides that whoever aids, abets, counsels, commands, induces or procures the commission of an offense against the United States is punishable as a principal, and whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

7. The following definitions apply to this Affidavit:

a. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. “Child pornography,” as defined in 18 U.S.C. § 2256(8)(A), is any visual depiction of sexually explicit conduct where the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct.

c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an

ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

e. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

f. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

g. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

h. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON TOR AND TOR HIDDEN SERVICES

8. Tor is a computer network designed to facilitate anonymous communication over the Internet. The Tor network does this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering conventional IP address-based

methods of identifying users ineffective. To access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle," which is available at www.torproject.org.¹ When a Tor user accesses a website, only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address, appears on the website's IP address log. Currently, there is no practical method to trace a user's actual IP address back through those Tor relay computers.

9. The Tor Network also makes it possible for users to operate websites, called "hidden services," in a manner that conceals the true IP address of the computer hosting the website. Like other websites, "hidden services" are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that conceal the computer server's location. Unlike standard Internet websites, a Tor-based web address is comprised of a series of 16 algorithm-generated characters, for example "asdlk8fs9dfiku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden-service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-

¹ Additional information outlining Tor and how it works is publicly accessible at www.torproject.org.

service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

BACKGROUND OF THE INVESTIGATION OF PAUL J. WILSON

10. In and before 2015, FBI agents investigated a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children. This bulletin board and website, known as “Playpen,” was a “dark web” bulletin board that was only accessible through Tor. The URL of Playpen changed frequently. Its URLs were a series of 16 characters and numbers that must be precisely entered, making it exceedingly unlikely that one would accidentally visit Playpen. Moreover, in order to access the bulletin-board service and/or advertise, distribute or receive child pornography, visitors of Playpen needed to register as users of the website.

11. In February 2015, after the Playpen server had been located and seized by law enforcement, this Court authorized the deployment of a Network Investigative Technique (“NIT”) on Playpen in an attempt to identify the actual IP addresses and other identifying information of computers used to access the website. Pursuant to that authorization, for a period in February and March 2015, each time any user logged into Playpen by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user’s computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing Playpen. This data included the computer’s actual IP address and other information.

Investigation of Playpen User “horatioalger” and Identification of WILSON

12. One such user of Playpen registered with a username of “horatioalger.” The profile page of user “horatioalger” indicated this user originally registered an account on Playpen on September 28, 2014. According to the user “horatioalger’s” profile, this user was a “Newbie Member” of Playpen. Further, according to the Statistics section of this user’s profile, the user “horatioalger” had been actively logged into Playpen for a total of 13 hours between the dates of September 28, 2014 and March 5, 2015.

13. According to data obtained from logs on Playpen, law enforcement monitoring, and the deployment of the NIT, on February 22, 2015, the user “horatioalger” with IP address 173.79.180.24 accessed the post entitled “Sofia NEW GIRL 2014” on Playpen. This post was accessed through the “Pre-teen Photos, Girls HC” section of the website. In my training and experience “HC” is short for “hardcore,” which in turn refers to depictions of penetrative or oral sex acts.

14. During the following additional sessions, the user “horatioalger” also browsed Playpen after logging in with a username and password, but the IP address was not collected during these sessions:

- (a) On February 26, 2015, the user “horatioalger” accessed a post that contained a link to a series of photographic images that depicted a pre-pubescent female child engaged in oral and vaginal sex with an adult male.
- (b) On February 26, 2015, the user “horatioalger” accessed a post that contained a link to a collage of photographic images that depicted pre-pubescent female children engaged in oral and vaginal sex with adult men.

15. Using publicly available websites, FBI agents were able to determine that the above IP address was operated by the ISP Verizon.

16. In March 2015, an administrative subpoena/summons was served to Verizon requesting information related to the user who was assigned to the above IP address at the time when “horatioalger” accessed Playpen. According to the information received from Verizon, the IP address above was assigned to WILSON at an address in Annandale, Virginia where he lived alone (the “WILSON RESIDENCE”). Annandale, Virginia is within the Eastern District of Virginia.

Execution of Search Warrant at the WILSON RESIDENCE and Interview of WILSON

17. On July 14, 2015, United States Magistrate Judge Michael S. Nachmanoff authorized a search warrant for the WILSON RESIDENCE.

18. On July 15, 2015, the search warrant was executed at the WILSON RESIDENCE and law enforcement personnel seized multiple items, including a desktop computer identified by the Seizing Agent as “black CPU/Server, Possibly Custom Built, Collected from Room A Next to Sliding Glass Door, Plugged In When Recovered” (the “black CPU”).

19. WILSON was not present at the WILSON RESIDENCE at the time the search warrant was executed. He was located later that day at his place of employment, a school (the “SCHOOL”) in Washington, D.C., where he worked as the Assistant Director of Information Technology. After FBI agents identified themselves and the reason for the interview, Wilson voluntarily agreed to be interviewed. WILSON admitted to viewing child pornography downloaded from the internet using Tor. WILSON acknowledged he had a problem with child pornography along with a degree of hopelessness regarding the matter. WILSON identified multiple websites he accessed via Tor to view and download child pornography.

20. During the interview WILSON identified multiple personal email addresses as his own, including but not limited to “paulj.wilson@gmail.com,” “paolo@dumpsternet.org,” “pauljwilson@dumpsternet.org,” and “paulj.wilson@dumpsternet.org.” WILSON identified “dumpsternet.org” as his personally owned domain name.

21. At the time of the interview, WILSON had already given notice of his intent to terminate his employment with the SCHOOL. His employment at the SCHOOL ended on the day of the search warrant.

Forensic Analysis of Computer Seized from WILSON RESIDENCE

22. A subsequent digital forensic review of the black CPU revealed seven hard drives contained within the computer housing. Numerous digital images of contraband child pornography were located on two of the hard drives contained within the black CPU, either in allocated or unallocated space.

23. The first hard drive in the black CPU, referred to here as “C1,” contained a computer application entitled “Pan” used to access files on the internet using “newsgroups.” Newsgroups are subscription-based news and information services covering an extremely wide variety of topics. Individual users “subscribe” to topics of interest and the program delivers the newest articles or postings for that topic. These articles or postings can be saved to the user’s computer in the form of “.msg” files. The articles and postings may contain digital files encoded into text. The newsgroup program decodes the digital files attached to the article or post, rendering them into a usable or viewable format for the user.

24. Additionally, hard drive “C1” contained evidence that WILSON had subscribed to newsgroups with titles suggestive of adult pornography, child pornography and child erotica. Examples include the following: “alt.binaries.picture.hussy,” “alt.binaries.picture.ls-series,”

“alt.binaries.pictures.erotica.schoolgirls,” “alt.binaries.picture.erotica.ls-series,”
“alt.binaries.pictures.bdcompany,” “alt.binaries.preadolescents,” “alt.binaries.pictures.newstar,”
“alt.binaries.pictures.nymphets,” and “alt.hipclone.sex.jailbait.” “Hussy,” “ls-series,”
“bdcompany,” “newstar,” “nymphets,” and “jailbait” are all known child pornography terms.
“LS” refers to “Lolita Studios” or “LS Models,” which refer to known child pornography series.
“bdcompany” refers to “Branded Dolls,” which likewise refer to known child pornography series.

25. Hard Drive “C1” also contained evidence that WILSON had downloaded “.msg” files containing or constituting child pornography from newsgroups on two specific dates, April 21, 2013 and August 01, 2013. These files were located in the article cache on hard drive “C1,” which signifies that the user deliberately downloaded them onto the computer. The files include the following:

(a) On April 21, 2013 the file

“_6adnTb5MvM0lZzWnZ2dnUVZ8qAAAAAA@giganews.com.msg” was saved to hard drive “C1” under the user profile “paolo.” It was downloaded from “alt.binaries.picture.ls-series” and it decoded to an image entitled “lsfan-001b-047.” The image depicted a minor female who is approximately between the ages of 10 and 12 years old. She is pictured nude, sitting in a blue chair with plants behind her. She is wearing a shell necklace. Her naked genitalia are clearly visible.

(b) On April 21, 2013 the file “3K-

dncCN5tGampzWnZ2dnUVZ7oCdnZ2d@giganews.com.msg” was saved to hard drive “C1” under the user profile “paolo.” It was downloaded from

“alt.binaries.picture.ls-series” and it decoded to an image entitled “lsp-001b-056.” The image depicted a minor female who is approximately between the ages of 8 and 10 years old. She is pictured nude, sitting on a white fur rug. She is wearing black and silver high heel shoes with a silver wrap around her waist. She is leaning back and her genitalia are clearly visible.

(c) On August 1, 2013 the file

“2pWdnbAW_5lTHBLUnZ2dnUVZ_ofinZ2d@gonamic.de.msg” was saved to hard drive “C1” under the user profile “root.” It was downloaded from “alt.binaries.picture.bdcompany” and it decoded to an image entitled “angelina095.” The image depicted a white female who is approximately between the ages of 9 and 12 years old. She is pictured nude squatting down with balloon in her hands. She is wearing silver high heel shoes. Her genitalia are clearly visible below the balloon.

(d) On August 1, 2013 the file

“MloFmR6VjiG0mWODBb1F@JBinUp.local.msg” was saved to hard drive “C1” under the user profile “root.” It was downloaded from “alt.binaries.picture.bdcompany” and it decoded to an image entitled “bd-hot_23.2.08-027.” The image depicted a female who is approximately between the ages of 8 and 10 years old. She is pictured nude squatting down with her back against a tree and one leg extended. Her genitalia is clearly visible as the focus of the image.

26. Additional forensic evidence on hard drive “C1” from both before and after the dates child pornography was downloaded to Hard Drive “C1” on April 21, 2013 and August 01,

2013 indicate that WILSON was the user of the computer. For example, digital files associated with the online media streaming application “Subsonic” were created and saved to Hard Drive “C1” on March 19, 2013. One such file located on Hard Drive “C1,” entitled “subsonic.properties,” was automatically generated by the Subsonic program. It included the statement, “Subsonic is a free, web-based media streamer, providing ubiquitous access to your music” and contained the information on the user’s account and preferences including, but not limited to, the following:

- (a) Identified “LicenseEmail” for the user’s account and preferences as
“paulj.wilson@gmail.com.”
- (b) Identified “UrlRedirectTrialExpires” date as 1366305325559. An open source UNIX computer time converter rendered this date as GMT April 18, 2013 5:15:26.559 PM.
- (c) Identified “SettingsChanged” date as 137357752876. An open source UNIX computer time converter rendered this date as GMT July 11, 2013 9:18:48.768 PM.

27. A digital file associated with the internet browser history of the Mozilla Firefox application was located on hard drive “C1” with a creation date of January 29, 2013. The file, entitled “places.sqlite” was automatically generated by the Mozilla Firefox program. It contained information on the user’s internet browser activity including, but not limited to, the following:

- (a) In excess of one hundred (100) browser history notations for
“mail.google.com” which reference “paulj.wilson@gmail.com.” Each of the identified “mail.google.com” browser history notations included a time and date stamp from March 29, 2014 through May 23, 2014.

(b) Six (6) browser history notations for “maps.google.com” which reference the location of the WILSON RESIDENCE. Each of the identified “maps.google.com” browser history notations included a time and date stamp from May 13, 2014 through May 14, 2014.

28. Hard drive “C1” also contained numerous thumbnail images of child pornography under the “Paolo” user profile.

29. The second hard drive labeled as “C2” was also found to contain numerous images of child pornography. As the images were previously deleted no download dates or file system location information was discovered. The recovered images were “carved” by a digital forensic tool specifically designed to locate deleted files on hard drives. Examples of the recovered child pornography included:

(a) Digital image entitled “Carved [3677696].jpeg” depicts a minor female who is approximately between seven (7) and nine (9) years of age nude in a squatted position. She is dressed in rabbit ears and a white fur cape. Her prepubescent genitalia are clearly visible. In the top corner of the images is a logo that reads “LS Models.” As noted above, “LS” refers to “Lolita Studios” or “LS Models,” which refer to known child pornography series.

(b) Digital image entitled “Carved [40558080].jpeg” depicts a minor female between five (5) and seven (7) years of age. She is mostly nude, wearing only white lace panties that she has pulled down to her mid-thigh. Her prepubescent genitalia are clearly visible. In the top corner of the images is a logo that reads “LS Models” followed by the internet address “www.ls-models.com.”

WILSON's Location During Child Pornography Downloads in 2013

30. The investigation further revealed that, at the time that WILSON used the black CPU to download child pornography files through a newsgroup program, he resided in Washington, D.C. As noted above, at the time that law enforcement seized the black CPU (which still contained the child pornography files), that black CPU was located in Annandale, Virginia. Accordingly, at some point between the 2013 child pornography downloads in Washington, D.C. and the 2015 seizure of the black CPU in Virginia, WILSON necessarily transported child pornography or caused it to be transported in interstate commerce.

31. Files on hard drive "C1" indicate that, when WILSON downloaded child pornography files from newsgroups, he did so from the server "news.giganews.com" under the username "slothor." The United States accordingly served legal process on GigaNews, Inc, a newsgroup service provider, for information related to WILSON's use of GigaNews to access newsgroups. The information provided by GigaNews included multiple accounts from various time periods linked to WILSON. In particular, GigaNews disclosed that between August 12, 2012 and August 18, 2013, a user named "slothor" with the email address slothor@dumpsternet.org received GigaNews service at the address of the SCHOOL in Washington, D.C. GigaNews also disclosed that between January and September 2010, and again between November 2011 and January 2012, WILSON received GigaNews service at the address of the SCHOOL under the name "Paul J. Wilson" and the email addresses paulj.wilson@gmail.com and paolo@dumpsternet.org.

32. In addition, in response to a subpoena, a representative of the SCHOOL informed me that WILSON lived on campus at the SCHOOL during the period covering April 21, 2013

and August 01, 2013—the dates on which WILSON used the black CPU to download child pornography through newsgroups. As noted above, the SCHOOL is located in Washington, D.C.

33. On April 16, 2018, I interviewed WILSON's former supervisor at the SCHOOL regarding WILSON's employment history and residence on the SCHOOL's property. An attorney representing the SCHOOL's parent organization was present for this interview. During this interview, WILSON's former supervisor told me that as part of his employment, WILSON lived on the property for multiple years prior to moving to the WILSON RESIDENCE in 2014. WILSON lived on the property as a form of financial remuneration in lieu of additional pay. WILSON lived alone in a one bedroom apartment off of the dormitory common room. WILSON's supervisor, who visited WILSON's apartment multiple times, described it as cluttered and messy with computer parts everywhere.

34. Legal process was served on the SCHOOL to obtain employment records related to WILSON's address of record. Among the documents provided were two "Personal Information Change Forms." The first form, dated April 15, 2008, identifies WILSON's address as a residence in Washington, D.C. and is signed by WILSON. The second form, dated March 05, 2010, identifies WILSON's address as that of the SCHOOL and is signed by WILSON.

35. Legal process was served on the owners of the apartment building that includes the WILSON RESIDENCE to obtain lease information for WILSON. Among the documents provided was the "Lease Application Agreement" for the WILSON RESIDENCE, dated March 14, 2014, which stated, among other things, that WILSON's "current residence" was the SCHOOL in Washington, D.C., and that the initial lease term at the WILSON RESIDENCE would commence on June 03, 2014.

36. The black CPU is a large computer that appears to be custom-built. Based on its size and weight, it is not mobile and cannot be easily transported. Here is a picture of the black CPU, taken at the WILSON RESIDENCE on the date of the search warrant execution:

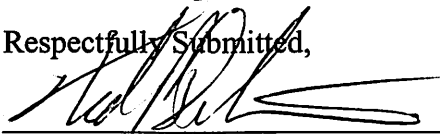


CONCLUSION

37. Based on the foregoing, your Affiant submits that there is probable cause to believe that between on or about April 21, 2013 and on or about July 15, 2015, PAUL J. WILSON transported or caused to be transported child pornography from Washington, D.C. to

Annandale, Virginia, which is in the Eastern District of Virginia, in violation of Title 18, United States Code, Section 2252(a)(1) and (b)(1) and 2.

Respectfully Submitted,



Ted P. Delacourt
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Subscribed to and sworn before me

This 14 day of December 2018.



/s/

Theresa Carroll Buchanan
United States Magistrate Judge

HONORABLE THERESA CARROLL BUCHANAN
UNITED STATES MAGISTRATE JUDGE